University of Alabama Office of Information Technology
125 Gordon Palmer Hall
Box 870346
Tuscaloosa, AL 35487-0346

July 15, 2019

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Notice of Data Breach

Brewer-Porch Children's Center (BPCC), a treatment program and residential facility for special-needs children, adolescents, and their families in Alabama, maintained a billing, employee, and state reporting system on an on-site proprietary server. After BPCC began using a new billing system, the server was taken offline and decommissioned. Prior to the server's anticipated disposal, The University of Alabama Office of Information Technology (OIT) conducted a security review of the server. During that review, on June 4, 2019, employees of OIT discovered that unauthorized login activity from outside the United States had occurred between October 24, 2009 and November 2, 2009. The University suspects that these credentials were obtained by brute force. Those unauthorized connections remained open until the server was rebooted on December 9, 2009. Although there was opportunity for access to personal information, including Social Security numbers, stored on the server, the University discovered no evidence that personal information, including Social Security numbers, was, in fact, accessed or used. The security review indicated there was no unauthorized access to the server after December 9, 2009.

The University's subsequent internal investigation concluded that between October 15-20, 2009, a more secure communications protocol was installed to assist with BPCC's server, which had to remain onsite at BPCC due to exceptionally slow network speed. The server was rebooted on October 22, 2009. It appears that the Access Control List (ACL) was not modified until a year later. The result of this oversight was the possibility for unauthorized connections over SSH, which may have permitted the 2009 successful unauthorized login activity. That ACL was modified in December of 2010, but as noted above, there was no successful unauthorized login activity after the server was rebooted on December 9, 2009.

According to The University of Alabama's records, there are two (2) Maryland residents who will be notified of the breach. Additionally, for your records, we have attached to this correspondence a sample of the notification letter these residents will receive.

In the decade since this incident occurred, The University of Alabama Office of Information Technology ("OIT") has implemented many mechanisms to minimize unauthorized access to sensitive information to the extent it is possible. OIT has redesigned the University's network, moving the vast majority of devices away from public IP addresses to protected private IP address spaces behind multiple layers of firewalls and Intrusion Detection/Prevention Systems. Network speeds have increased to the point where it is no longer necessary to keep servers at remote sites, and most have been consolidated in OIT's data center. OIT has implemented multiple types of network protection, such as extreme segmentation, Virtual Routing and Forwarding, VLAN isolation, and Access Control Lists. OIT regularly scans servers for known vulnerabilities and monitors servers for unauthorized file modifications through a file integrity monitoring system. OIT also monitors servers with anti-malware software and monitors servers for suspicious behavior. OIT has implemented robust log aggregation and event correlation systems to help detect and alert employees of potential malicious activities on UA's networks and servers. OIT now works with a managed security service provider that continually monitors logs from firewalls and intrusion detection systems, and alerts OIT personnel when there are indications of malicious activity. OIT has developed policies and procedures designed to ensure that industry-standard best practices are followed, to make sure that our networks and systems are as secure as possible.

Sincerely,

Ashley Ewing
Chief Information Security Officer
The University of Alabama